UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

HEIDI MATHIASEN, individually and on behalf of all others similarly situated, Plaintiff, v. THOMPSON COBURN LLP, Defendant.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Heidi Mathiasen ("Plaintiff"), individually and on behalf of all others similarly situated, sues Defendant Thompson Coburn LLP ("Thompson Coburn" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

I. INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the "Data Breach"), which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") of Plaintiff and other current and former patients of Defendant's client Presbyterian Healthcare Services ("Presbyterian"). This Data Breach occurred between May 28 and 29, 2024.

2. The Private Information compromised in the Data Breach included certain personal or protected health information of Presbyterian's patients, including Plaintiff. This Private Information included but is not limited to "name, medical record number, patient account number,

prescription/treatment information, clinical information, and medical provider information." See Notice Letter, Exhibit A.

3. The Private Information was "viewed or taken" by cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals. According to Defendant's report to the Health and Human Services Office of Civil Rights, 305,088 individuals were affected.[1]

4. The Data Breach resulted from Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which they were entrusted for treatment.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was subjected to unauthorized access by an unknown third party and precisely what information was accessed.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Defendant, through its employees, disregarded the rights of Plaintiff and Class Members (defined below) by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (*last accessed* November 11, 2024).

protected against unauthorized intrusions. Defendant also failed to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information and failed to take standard and reasonably available steps to prevent the Data Breach.

8. In addition, Defendant's employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant's employees (presumably in the IT department) properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes. These crimes include using Class Members' information to obtain government benefits, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. Because of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiff sues Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of third-party-beneficiary contract, and (iv) unjust enrichment.

II. PARTIES

16. Plaintiff Heidi Mathiasen is and at all times mentioned herein was an individual citizen of New Mexico, residing in the city of Española.

17. Defendant Thompson Coburn LLP is a Missouri limited liability partnership with its principal place of business located at One U.S. Bank Plaza, Suite 3500, St. Louis, Missouri 63101.

18. Defendant's registered agent is Roman P. Wuller, located at One U.S. Bank Plaza, Suite 2700, St. Louis, Missouri 63101.

III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

20. This Court has general personal jurisdiction over Defendant because Defendant has its principal place of business within this District.

21. Venue is proper in this Court under 28 U.S.C. §1391(b) because Defendant conducts business in this District and because a substantial part of the acts or omissions giving rise to this action occurred within this District.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

22. Defendant is a St. Louis-based law firm that employs more than 400 attorneys at offices throughout the United States.

23. Defendant represents Presbyterian Healthcare Services in various matters. In connection with that representation, Presbyterian entrusted Defendant with the PHI of hundreds of thousands of patients, including Plaintiff.

24. In the ordinary course of receiving healthcare services from Presbyterian, each patient must provide (and Plaintiff did provide) Presbyterian with sensitive, personal, and private information, such as his or her contact information, date of birth, and medical history.

25. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Presbyterian safely, confidentially, and in compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA").

26. The patient information held by Defendant in its computer system and network included the Private Information of Plaintiff and Class Members.

THE DATA BREACH

27. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

28. According to the Notice letter Defendant sent to Plaintiff (Exhibit A),

> **What Happened?** On May 29, 2024, Thompson Coburn became aware of suspicious activity within our network. We immediately launched an investigation with the assistance of third-party forensic specialists. The investigation determined that certain information stored within our environment was viewed or taken by an unauthorized actor between May 28, 2024, and May 29, 2024. A detailed review of the affected files began and through that review, we determined that certain of your information was contained within those files.
>
> **What Information Was Involved?** Our review determined that the information that may have been involved includes: your name, medical record number, patient account number, prescription/treatment information, clinical information, and medical provider information.

29. The U.S. Department of Health and Human Services requires, "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[2] Further, if "the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HSS.[3]

30. Defendant cannot claim it was unaware of the HHS notification requirements as it complied (at least in part) with those requirements.

31. Plaintiff's notice letter was dated November 6, 2024—around five months after Defendant became aware of the Data Breach.

32. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to its client, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

---

[2] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary* (Feb. 27, 2023) https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed June 10, 2024) (emphasis added).
[3] *Id.*

33. Plaintiff and Class Members provided their Private Information to Presbyterian with the reasonable expectation and mutual understanding that Presbyterian's vendors would comply with their obligations to keep such information confidential and secure from unauthorized access.

34. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches in both the healthcare industry and the professional services industry preceding the date of the breach.

35. In 2023, a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[4] Of the 2023 recorded data breaches, 809 of them, or 25%, were in the medical or healthcare industry.[5] The 809 reported breaches reported in 2023 exposed nearly 56 million sensitive records, compared to only 343 breaches that exposed just over 28 million sensitive records in 2022.[6]

36. 2023 also saw 308 data breaches in the professional services sector.[7]

37. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

[4] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited September 24, 2024).
[5] *Id.*
[6] *Id.* at 11, Fig.3.
[7] *Id.*

38. Thompson Coburn advertises itself to potential clients as experienced in cybersecurity matters and able to "rapidly respond to claims, threatened litigation, and investigations related to data security breaches."[8]

39. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

40. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

41. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[9] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

---

[8] Defendant Thompson Coburn, Litigation and Data Breach, *available at* https://www.thompsoncoburn.com/services/practices/cybersecurity/litigation-and-data-breach (last visited Nov. 12, 2024).

[9] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 19, 2024).

[10] *Id.*

42. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions also clarify the measures businesses must take to meet their data security obligations.

44. Defendant failed to properly implement basic data security practices.

45. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

46. Defendant was always fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

47. As shown above, experts studying cyber security routinely identify custodians of healthcare data as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

48. Several best practices have been identified that a minimum should be implemented by professional services providers like Defendant, including, but not limited to, educating all

employees; using strong passwords; creating multi-layer security, including firewalls, antivirus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data; and limiting which employees can access sensitive data.

49. Other best cybersecurity practices that are standard in the professional services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

50. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including, without limitation, PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

51. These foregoing frameworks are existing and applicable industry standards in the healthcare and professional services industries, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

DEFENDANT'S CONDUCT VIOLATES HIPAA AND REVEALS ITS INSUFFICIENT DATA SECURITY

52. Defendant is a Business Associate of Presbyterian within the meaning of the Health Insurance Portability and Accountability Act ("HIPAA"). 45 CFR § 160.103.

53. HIPAA rules require Business Associates such as Defendant to contract with their healthcare-provider clients to "Use appropriate safeguards . . . to prevent use or disclosure of" the clients' PHI. 45 CFR § 164.504(e).

54. Defendant's Data Breach resulted from insufficient safeguards that violated HIPAA and Defendant's contract with Presbyterian.

V. DEFENDANT'S BREACH

55. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's client's protected health data employed reasonable security procedures; and/or

e. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304, definition of "encryption").

56. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing malignant computer code, and inadequately trained employees who opened files containing malignant computer code, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

57. Plaintiff and Class Members now face an increased risk of fraud and identity theft.

DATA BREACHES PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

58. Data Breaches such as the one experienced by Defendant's patients are especially problematic because of the disruption they cause to the daily lives of victims affected by the attack.

59. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[11]

60. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (possibly an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[12]

61. Theft of Private Information is gravely serious. PII/PHI is a valuable property right.[13] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

62. Theft of PHI is also gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get

[11] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited May 21, 2024) ("GAO Report").

[12] Federal Trade Commission, *What To Do Right Away* (2024), *available at* https://www.identitytheft.gov/Steps (last visited August 19, 2024).

[13] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[14] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

63. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

64. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

65. There is a strong probability that all the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

[14] *See* Federal Trade Commission, *Medical Identity Theft*, *available at* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited May 21, 2024).

66. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[15] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

67. Healthcare data is especially prized by data thieves. The National Association of Healthcare Access Management reports, "[p]ersonal medical data is said to be more than ten times as valuable as credit card information."[16]

68. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $300 and up.[17]

69. The value of Plaintiff's and the proposed Class's PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

70. It can take victims years to spot identity or PHI theft, giving criminals plenty of time to milk that information for cash.

71. One such example of criminals using PHI for profit is the development of "Fullz" packages.

---

[15] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited May 21, 2024).

[16] Laurie Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*, NAHAM Connections, *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information (last visited August 30, 2024).

[17] Paul Ducklin, *FBI "ransomware warning" for healthcare is a warning for everyone!*, Sophos (Oct. 29, 2020) *available at* https://news.sophos.com/en-us/2020/10/29/fbi-ransomware-warning-for-healthcare-is-a-warning-for-everyone/ (last visited September 24, 2024).

72. Cyber-criminals can cross-reference two sources of PII or PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

73. The development of "Fullz" packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PHI is being misused, and that such misuse is traceable to the Data Breach.

74. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

VI. PLAINTIFF'S EXPERIENCE

75. Plaintiff Heidi Mathiasen is and at all times mentioned herein was an individual citizen of New Mexico, residing in the city of Española.

76. Plaintiff used Presbyterian's services, requiring her to provide her Private Information to Presbyterian and, indirectly, to Defendant.

77. Plaintiff received notice of the Data Breach around November 6, 2024, informing her that her sensitive information was part of Defendant's Data Breach, including her "name, medical record number, patient account number, prescription/treatment information, clinical information, and medical provider information"—which includes PHI. Exhibit A.

78. Plaintiff reasonably expected and understood that Presbyterian's vendors, including Defendant, would take, at a minimum, industry standard precautions to protect, maintain, and safeguard her Private Information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to the same.

79. Plaintiff is very careful about sharing her sensitive PII and PHI. she has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff also stores any documents containing her sensitive information in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

80. Because of the Data Breach and at the recommendation of Defendant and its Notice, Plaintiff made reasonable efforts to mitigate the effect of the Data Breach, including, but not limited to, researching the Data Breach and reviewing financial statements.

81. Plaintiff has spent much time responding to the dangers from the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and recreation.

82. Plaintiff is especially alarmed by the amount and type of stolen or accessed PII and PHI listed on Defendant's notice letter. Despite Defendant providing that list, she cannot be sure whether more of her PII or PHI was exfiltrated.

83. Plaintiff knows that cybercriminals often sell Private Information, and that her PII or PHI could be abused months or even years after a data breach.

VII. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

84. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered up to 12 months of inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

85. The credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

86. Defendant's credit monitoring advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

87. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

88. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

89. Plaintiff was damaged in that her Private Information is in the hands of cyber criminals.

90. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

91. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

92. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, and similar identity theft.

93. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

94. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

95. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

96. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

97. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

98. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

99. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

100. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

VIII. CLASS ACTION ALLEGATIONS

101. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

102. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons whose Private Information was compromised because of the May 28-29, 2024 Data Breach (the "Class").**

103. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

104. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 23 of the Federal Rules of Civil Procedure.

105. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiff now, but Defendant has provided notice to the Health and Human Services Office of Civil Rights that 305,088 individuals were affected.

106. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach adhered to industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiff and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's conduct was *per se* negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant was unjustly enriched;

m. Whether Defendant failed to provide notice of the Data Breach promptly; and

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

107. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class

Members, and no defenses are unique to Plaintiff. Plaintiff's claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

108. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

109. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

110. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

111. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

112. Likewise, issues that will arise in this case are appropriate for class certification because such issues are common to the Class, the resolution of which would advance matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable considering best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

113. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

IX. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

114. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

115. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting

their Private Information and keep it from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

116. By collecting and storing Plaintiff's and Class Members' sensitive data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

117. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

118. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

119. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

120. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Failing to store Class Members' Private Information in an encrypted state;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect timely that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

121. As a direct and proximate result of Defendant's breaches, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the compromise, publication, and/or theft of their Private Information;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession;

f. future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and

g. the diminished value of Defendant's services they received.

122. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

123. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

124. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

SECOND COUNT
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and All Class Members)

125. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

126. Defendant entered into one or more written contracts with its Presbyterian to provide legal services.

127. Defendant agreed, in part, to implement adequate security measures to safeguard the PHI of Plaintiff and Class Members and to timely and adequately notify them of any Data Breach.

128. These contracts were made expressly for the benefit of Plaintiff and Class Members, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its Presbyterian. Defendant knew that, if it were to breach these contracts with Presbyterian, Presbyterian's patients—Plaintiff and Class Members—would be harmed.

129. Defendant breached the contracts it entered into with Presbyterian by, among other things, (i) failing to use reasonable data security measures, (ii) failing to implement adequate

protocols and employee training sufficient to protect Plaintiff's PII from unauthorized disclosure to third parties, and (iii) failing to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

130. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its client, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result of Defendant's breach.

131. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

THIRD COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

132. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

133. Under the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

134. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

135. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

136. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

137. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that

its breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

138. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above seeks the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiff and their counsel to represent the Class, and finding that Plaintiff is a proper representative of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For an order directing Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre- and post-judgment interest on any amounts awarded; and

i. Any other relief that this court may deem just and proper.

XI. JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: November 13, 2024

Respectfully submitted,

/s/ *Daniel F. Harvath*

Daniel F. Harvath,
Missouri Bar No. 57599MO
dharvath@harvathlawgroup.com
HARVATH LAW GROUP, LLC
75 W. Lockwood, Suite #1
Webster Groves, MO 63119
(314) 550-3717

Leigh S. Montgomery*
Texas Bar No. 24052214
lmontgomery@eksm.com
EKSM, LLP
1105 Milford Street
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

ATTORNEYS FOR PLAINTIFF
(* denotes *pro hac vice* forthcoming)